REMARKS

This Amendment is submitted in response to the Office Action dated June 30, 2005, having a shortened statutory period set to expire September 30, 2005. Proposed amendments are submitted for Claims 1, 3, 6, 8, 11 and 13, and new Claims 16-18 are proposed. Upon entry of the proposed amendments, Claims 1-18 will now be pending.

Objections to the Drawings

At page 2 of the present Office Action, Figure 7a is objected to for failing to clearly mark "child key 1.2" as an element "70." The replacement sheet shows all child keys in Figure 7a as elements "70," and thus Applicants respectfully request that the objection be withdrawn.

Objections to the Specification

At page 3 of the present Office Action, Page 13 was objected to for two typographical errors, which are corrected in the present amendment. Thus, Applicants respectfully request that this objection be withdrawn.

Rejections under 35 U.S.C. § 103

At page 3 of the present Office Action, Claims 1-3, 5-8, 10-13 and 15 are rejected under 35 U.S.C. § 103(a) as being unpatentable over TCPA's "Main Specification Version 1.0" ("*TCPA*") in view of *Challenger et al.* (U.S. Patent No. 6,266,742 B1 – "*Challenger*"). On page 6 of the present Office Action, Claims 4, 9 and 14 are rejected under 35 U.S.C. § 103(a) as being unpatentable over *TCPA* and *Challenger* in further view of *Deshpande et al.* (U.S. Patent No. 5,893,103 – "*Deshpande*"). In light of the present amendments, Applicants respectfully traverse these rejections.

With regards to exemplary Claim 1, the cited art does not teach or suggest determining a cycle time required to re-store an evictable cryptology key by cycle time is determined by **calculating a number of generations to a nearest ancestor that is required to unwrap said least expensive evictable cryptology key**, said nearest ancestor being from a plurality of non-evicted remaining cryptology keys in the computer module," as supported, *inter alia*, on pages 8-9 of the present specification.

This feature is described mathematically on Page 12 of the specification, wherein:

Ki = each least TPM key
S = all private keys previously stored in the TPM RAM
Kj = evicted private TPM key
N = newly loaded private TPM key,

then the minimum impact on loading future TPM private keys is the minimum generational distance D_{min} to the nearest storage key related to the replaced TPM private key, where

$$D_{min} = \left[\sum_{I}^{i} D(Ki, S - Kj + N) \right]_{min}$$

Challenger teaches a method for determining which value to replace in cache. Part of the equation taught on column 4 of *Challenger* uses "a", which is "the expected time between successive requests" for an object (*Challenger*, col. 4, lines 60-61). However, there is no teaching or suggestion that this time is based on "calculating a number of generations to a nearest ancestor cryptology key that is required to unwrap said least expensive evictable cryptology key."

Similarly, in the passages from *Challenger* cited in the present Office Action (including col. 1, lines 28-32 and col. 3, lines 52-67), *Challenger* teaches that caching of objects may depend on "the frequency with which an object is accessed, object size, the time to calculate an

object, or the time to fetch the object from a remote location, and the lifetime (i.e., time between updates) of an object." (*Challenger*, col. 1, lines 28-32.) The Examiner cites this passage as disclosing "as obvious that fact that calculating the time necessary to fetch an object would include the time it takes to fetch the ancestors of which the object depends upon in the hierarchal data structure." (Page 5, lines 18-20 of the present Office Action.)

Applicants respectfully traverse Examiner's contention. The cited art does not teach or imply "calculating a number of generations to a nearest ancestor cryptology key that is required to unwrap said least expensive evictable cryptology key" because the cited art never mentions or implies considering ancestors at all, much less ancestor objects used to unwrap children objects. It is axiomatic that the prior art must teach or suggest all of the limitations found in the presently presented claim. If it is the Examiner's position that "calculating a number of generations" is "commonly known" when determining cycle time in the context of the claimed invention, then Applicants traverse this position, and respectfully request that the Examiner provide documentary evidence of such "well known" art, per the requirements of MPEP § 2144.03.

Note that Claims 6 and 11 include the same features as Claim 1.

With regards to exemplary Claim 3 (and analogous Claims 8 and 13), the cited art does not teach or suggest "wherein an expense to re-load an evictable cryptology key is determined by both an expense to reload a child evictable cryptology key as well as an expense to re-load any ancestor cryptology keys of the child evictable cryptology key," which is supported, *inter alia*, on page 4 of the present specification.

With regards to new exemplary Claim 16 (and analogous new Claims 17-18), the cited prior art does not teach or suggest the feature, supported, *inter alia*, by Figure 7c of the present specification, of "prior to evicting a parent cryptology key, determining how many child cryptology keys of the parent cryptology key will be disabled by the evicting of the parent cryptology key; and evicting from a plurality of parent cryptology keys a parent cryptology key that has been determined to affect fewer child cryptology keys that other parent cryptology keys in the plurality of parent cryptology keys."

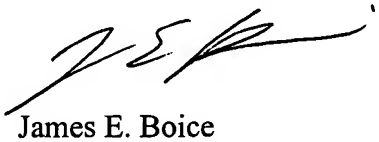
CONCLUSION

As the cited art does not teach or suggest all of the claimed features, Applicants now respectfully request a Notice of Allowance for all pending claims.

Applicant further respectfully requests the Examiner contact the undersigned attorney of record at 512.343.6116 if such would further or expedite the prosecution of the present Application.

No extension of time for this response is believed to be necessary. However, in the event an extension of time is required, that extension of time is hereby requested. Please charge any fee associated with an extension of time as well as any other fee necessary to further the prosecution of this application, including fees (if any) required by the addition of new claims, to **LENOVO DEPOSIT ACCOUNT No. 50-3533.**

Respectfully submitted,



James E. Boice
Registration No. 44,545
DILLON & YUDELL LLP
8911 North Capital of Texas Highway
Suite 2110
Austin, Texas 78759
512.343.6116

ATTORNEY FOR APPLICANT(S)